

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF OREGON

CAROLE BIONDELLO,)	
)	
Plaintiff,)	Civ. No. 05-6263-HO
)	
)	
v.)	ORDER
)	
INTEGRETEL, INC., INFORMATION)	
SERVICES 900 LLC, NATIONAL)	
COMMUNICATIONS TEAM, INC., LO/AD)	
COMMUNICATIONS CORP., AND NICHOLAS)	
LOADER,)	
)	
Defendants.)	
)	

Plaintiff Carole Biondello brings this action against defendants Integretel, Inc., Information Services 900 LLC, National Communications Team, Inc., LO/AD Communications Corp., and Nicholas Loader alleging unlawful interception and use of wire and electronic communications in violation of 18 U.S.C. § 2511. Plaintiff seeks statutory and punitive damages pursuant to 18

U.S.C. § 2520. Plaintiff alleges that she is a computer user whose electronic communications were unlawfully intercepted and used by defendants who are in the modem hijacking business. Defendants Integretel, Inc. and Information Services 900 LLC move to dismiss. Defendants National Communications Team, Inc., LO/AD Communications Corp., and Nicholas Loader join the motion to dismiss.¹

ALLEGATIONS IN THE COMPLAINT

Defendant Information Services 900 owns the faq900.com internet domain. Defendant National Communications Team operated a nationwide 900 network. Defendant Nicholas Loader is or was the president of National Communications Team. Defendant Integretel is an internet billing company and is affiliated with Information Services 900 and billed for National Communications Team.

Defendants are in the modem hijacking business. To find victims, they set traps on the internet. When an unsuspecting user falls into one of these traps such as a pop-ad, a dialer program is loaded onto the user's computer.

The program takes control of the user's computer modem, causing it to call a 900 telephone number without the user's knowledge or permission. Integretel bills for these unauthorized calls by inserting the charges (typically \$40) on the telephone bill for the telephone number associated with the hijacked computer. The ostensible creditor is listed as faq900.com or

¹To the extent defendants National Communications Team, Inc., LO/AD Communications Corp., and Nicholas Loader move to join in the motion to dismiss, the motion (#14) is granted.

faq900.comZZ or InfoServicZZ or Information Service or other variations thereof.

Complaint (#1) ¶ 3.

In or about November of 2004, plaintiff found a charge for \$40 from Integretel on her Qwest phone bill for an alleged two minute telephone call to 900-444-0319. The bill stated that the call was being billed on behalf of "Information Service." Plaintiff searched the internet for Integretel and found dozens of complaints against the company. Plaintiff called Integretel to complain and the company agreed to remove the charge. Plaintiff later received a credit from Integretel for the \$40 charge and additional \$40 credit from Qwest.

The complaint also lists anonymous examples of complaints against Integretel. Plaintiff then alleges that defendants, working together in a conspiracy, are behind this scam. "One or more defendants cause the dialer programs to be secretly downloaded onto the computers of unsuspecting internet users. The dialer programs cause the computers to make telephone calls to a 900 number for which the telephone number associated with [that] computer is billed." Complaint at ¶ 14. The complaint then lists three anonymous complaints to "illustrate how the scheme works."

Plaintiff then alleges that when victims call Integretel, Integretel will "typically begin by insisting that the calls were authorized and then offer a 50% discount while threatening to send the remainder of the bill to collection agency. If the caller is

persistent enough, Integretel will typically agree to waive the charges." Complaint at ¶ 16. Plaintiff then lists three more anonymous "postings as illustrative."

Plaintiff continues by alleging that the faq900.com web site provides further evidence as to the fraudulent nature of the business as it is mainly devoted to answering frequently asked questions of how and why unauthorized charges have mysteriously appeared on the user's telephone bill. Plaintiff then lists more anonymous internet postings.

Plaintiff alleges that the scheme is similar to ones successfully prosecuted by the Federal Trade Commission that included Integretel, National Communications Team, LO/AD and Nicholas Loader as defendants.

Plaintiff then devotes five paragraphs to explaining Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Plaintiff alleges that defendants "intercepted plaintiff's electronic and wire communications for the purpose of committing tortious acts-unfair and deceptive practices-in violation of the consumer protections laws of the United States and Oregon." Complaint at ¶ 25. Specifically, plaintiff alleges that defendants intercepted plaintiff's communications for purposes of fraud in violation of the mail and wire fraud statutes and state statutes prohibiting fraud by deception. Accordingly, plaintiff alleges that defendants violated 18 U.S.C. § 2511.

DISCUSSION

Plaintiff's complaint is deficient in that it doesn't allege the facts related to the apparent scheme to defraud her. Nowhere in the complaint is an allegation that defendants, without authorization, loaded a program on her computer that caused her computer to make unauthorized calls via her modem. There are only implications that this occurred by reference to anonymous complaints of computer users. The only allegations specifically related to fraud committed against plaintiff are those related to her receiving a 40 dollar charge on her phone bill for which she was reimbursed 80 dollars. Accordingly, the motion to dismiss is granted, but with leave to plead facts pertinent to the alleged fraud suffered by plaintiff.

Defendants move to dismiss contending the complaint fails to allege any facts entitling plaintiff to relief and that the cause of action the complaint purports to allege does not exist.

Plaintiff purports to allege a cause of action under Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510-22 for modem hijacking.

Any person who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication shall be

subject to suit. 18 U.S.C. § 2511(1)(a).² "Intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. 18 U.S.C. § 2510(4). "Contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8). Before an interception can exist, there must be some form of active surveillance. Greenfield v. Kootenai County, 752 F.2d 1387, 1389 (9th Cir. 1985). "It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C. § 2511(2)(d).

Defendants first argue that complaint should be dismissed because it fails to allege any of the defendants "hijacked"

²Any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate. 18 U.S.C. § 2520. It appears that plaintiff is using this provision as her cause of action rather than a more appropriate fraud action because she has no actual damages and Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510-22 provides for statutory and punitive damages.

plaintiff's modem. As noted above, the complaint relates tales of other computer users who were subjected to unauthorized programs loaded onto their computers and that such programs caused their modems to place calls to a 900 service. The complaint is lacking allegations in this regard with respect to any computer and modem plaintiff may own and use. The motion is granted in this regard without prejudice to filing an amended complaint.

Defendants next argue that they cannot be found to violate 18 U.S.C. § 2511 because there are no allegations that they acquired the contents of communications. Devices that reveal only the origin or destination of phone calls, and not the content, do not violate Title III. cf. United States v. Tutino, 883 F.2d 1125, 1140-41 (2nd Cir. 1989) (Unlike telephone wiretaps, duplicate paging devices reveal only numbers, not the content of conversation. In this way they are similar to pen registers. Because it is impossible to tell from the clone beeper whether a conversation even took place, much less the content of any conversation that might have taken place, traditional minimization requirements of 18 U.S.C. § 2518(5), do not apply). Defendants maintain that because plaintiff has not alleged that defendants eavesdropped on the substantive content of plaintiff's communications, the complaint should be dismissed.

Plaintiff argues that defendants intercepted their own electronic communications with their victims for criminal and

tortious purpose. Plaintiff further argues defendants did acquire the contents of the communication which led to the telephone charges as well as "the contents of whatever other communications the dialer program caused plaintiff's computer to send to defendants' computer and receive from defendants' computers." Plaintiff's Memorandum in Opposition to Motion to Dismiss (#16) at p. 15. Plaintiff does not allege what the contents of the communications intercepted were. Plaintiff argues that defendants "have to 'intercept' the content of the message from the user's computer to be able to provide that computer with the supposedly requested information or link the user's computer to the web site which provides the information content that defendants contend the users have agreed to access." Memo at p. 4. Plaintiff also contends that "They also intercept the content of the internet web site which their computer(s) provide in response to the victims' (unwitting) use of defendants' dialer program." Id. However, the complaint still fails to allege the actual content defendants have intercepted. Moreover, the complaint makes clear that it is not the contents of the communication that defendants are alleged to intercept for the purpose of committing any criminal or tortious act, but rather the call and duration of the call itself regardless of the content.

While it appears that, at best, plaintiff can only allege that defendants transmitted unwanted messages (rather than intercepted

them) and intercepted information about the communication such as telephone line number, plaintiff is allowed to amend the complaint to allege more facts regarding interception and content. Whether the content intercepted can qualify as prohibited interception for purposes of the statute is probably better tested on summary judgment, once the facts regarding the communication between plaintiff's computer and the 900 service are discovered.³ The amended complaint should more clearly spell out the role that each defendant played in the scheme to defraud plaintiff (fraud being the underlying tortious act). Fraud must be plead with particularity.

Defendants next argue that the complaint fails to state a claim under Title III because it does not allege that they engaged in any "active surveillance" of plaintiff. This is a rehash of the argument that no communication itself was intercepted. If plaintiff can allege facts demonstrating interception of electronic communications then it would appear that the allegations that defendants surreptitiously placed a dialer program on plaintiff's

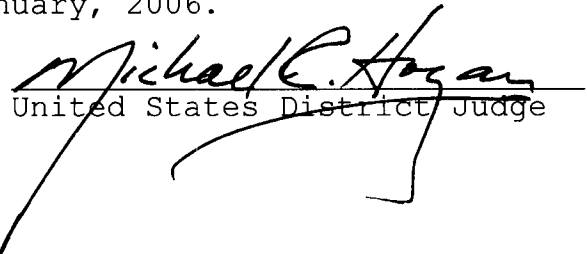
³Defendants also argue that the complaint must also allege that the defendants have intercepted the contents of a communication using a device distinct from the means of communication. Defendants continue that since the means of communication (the victim's computer with the alleged unauthorized dialer program) also is the device used for interception then no violation can occur because it only shows transmission of a communication and not interception. However, plaintiff could prove facts demonstrating that the dialer program combined with cookies left on plaintiff's computer is a device used to intercept communications from a computer for a fraudulent purpose. Moreover, there may be facts demonstrating that such a device exists through defendants' servers and storage devices that provide information services.

computer (assuming plaintiff will allege this as well) will suffice to demonstrate active surveillance if the purpose of the program was to intercept communications originating from plaintiff's computer.

CONCLUSION

For the reasons stated above, defendants National Communications Team, Inc., LO/AD Communications Corp., and Nicholas Loader's motion to join defendants Integretel, Inc. and Information Services 900 LLC motion to dismiss (#14) is granted. Defendants Integretel, Inc. and Information Services 900 LLC's motion to dismiss is granted. Plaintiff shall have 30 days to file an amended complaint addressing the deficiencies noted above.

DATED this 5th day of January, 2006.


United States District Judge